AU/ACSC/185/1999-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

ORGANIZING JOINT FORCES FOR INFORMATION OPERATIONS: THE VIABILITY OF A JOINT FORCE INFORMATION OPERATIONS COMPONENT COMMANDER

by

Jeffrey D. Seinwill, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Douglas G. Drake

Maxwell Air Force Base, Alabama

April 1999

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01041999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Organizing Joint Forces for Information Operations: The Viability of a Joint Force Information Operations Component Commander	**Contract or Grant Number**
	Program Element Number
Authors Seinwill, Jeffrey D.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Air Command and Staff College Air University Maxwell AFB, AL	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
A number of sources advocate creating a separate information component headed by a joint force information operations component commander (JFIOCC) as the best way to integrate information operations (IO) into joint forces. Though attractive on the surface, detailed investigation demonstrates that the JFIOCC is not a viable structure for joint force IO. The JFIOCC concept goes against the long-established principles of war. Specifically, structuring IO under a JFIOCC violates the principles of unity of command and simplicity. Another problem with creating a JFIOCC is the potential isolation of IO from other assets within the theater, reducing synergy. Concentrating joint force IO in a JFIOCC construct fails to recognize that information operations can be conducted on a global scale. The joint force must recognize its vulnerability to information attack from beyond its area of responsibility and the vulnerability of forces located outside the theater. The research concludes by offering an overview of alternative structures for integrating IO into joint forces.

Subject Terms

Document Classification unclassified	**Classification of SF298** unclassified

Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 52	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/1/99	White Paper

4. TITLE AND SUBTITLE
Organizing Joint Forces for Information Operations: The Viability of a Joint Force Information Operations Component Commander

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Jeffrey D. Seinwill, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This paper entitled "Organizing Joint Forces for Information Operations: The Viability of a Joint Force Information Operations Component Commander" was written by Major Jeffrey D. Seinwill, USAF while attending the Air Command and Staff College. A number of sources advocate creating a separate information component headed by a joint force information operations component commander (JFIOCC) as the best way to integrate information operations (IO) into joint forces. Though attractive on the surface, detailed investigation demonstrates that the JFIOCC is not a viable structure for joint force IO. The JFIOCC concept goes against the long-established principles of war. Specifically, structuring IO under a JFIOCC violates the principles of unity of command and simplicity. Another problem with creating a JFIOCC is the potential isolation of IO from other assets within the theater, reducing synergy. Concentrating joint force IO in a JFIOCC construct fails to recognize that information operations can be conducted on a global scale. The joint force must recognize its vulnerability to information attack from beyond its area of responsibility and the vulnerability of forces located outside the theater. The research concludes by offering an overview of

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Operations, Joint Forces	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Acknowledgements

This report is the result of the invaluable assistance of a number of people. The first thanks must go to Lieutenant Colonel Randall Scott, USA, and his staff at the Armed Forces Staff College. Their outstanding presentation of the evolving world of information operations through the Joint Information Staff and Operations Course piqued my professional and personal interest in the field. When the time came to select a topic for this project, a topic related to information operations was a natural choice.

The Air Force Doctrine Center research topic list was helpful in narrowing my project, and Lieutenant Colonel Mike "Dutch" Dietvorst was invaluable in pointing me in a productive direction and in narrowing the topic. His assistance making the contacts required to get the most current data regarding the fast-changing IO field was invaluable.

Mr. W. Darrel Phillips of the Air Force Judge Advocate General School went above and beyond the call of duty to make arrangements to allow Air Command and Staff College and Air War College students to participate in the Legal Aspects of Information Operations Symposium 99-A. The information I gleaned from the symposium was invaluable to this effort and will continue to serve me well in the future.

Finally, I must thank Lieutenant Colonel Doug Drake, my faculty research advisor. He combined valuable guidance with welcome latitude to conduct the research throughout this project. Whatever value the finished product has is due in large part to him.

Abstract

A number of sources advocate creating a separate information component headed by a joint force information operations component commander (JFIOCC) as the best way to integrate information operations (IO) into joint forces. Though attractive on the surface, detailed investigation demonstrates that the JFIOCC is not a viable structure for joint force IO. The JFIOCC concept goes against the long-established principles of war. Specifically, structuring IO under a JFIOCC violates the principles of unity of command and simplicity. Another problem with creating a JFIOCC is the potential isolation of IO from other assets within the theater, reducing synergy. Concentrating joint force IO in a JFIOCC construct fails to recognize that information operations can be conducted on a global scale. The joint force must recognize its vulnerability to information attack from beyond its area of responsibility and the vulnerability of forces located outside the theater. The research concludes by offering an overview of alternative structures for integrating IO into joint forces.

Chapter 1

Genesis of a Concept

Victory smiles upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

-- General Giulio Douhet

Setting the Stage

Information superiority will almost certainly be a key to victory in future conflicts. As the twentieth century draws to a close, we look back at a century that has seen rapid evolution in the conduct of warfare. Air and space forces, unknown at the outset of the century, were vital partners in the successes of Operation Desert Storm. The inclusion of what are now known as information operations during the campaign in the Persian Gulf also demonstrated the likely direction of future wars. The publication of the first joint doctrine of information operations (IO) in October 1998 demonstrates the level of attention this area of military operations is receiving.[1]

This attention is clearly understandable from the perspective of the United States. American society depends upon all sorts of modern technology for many capabilities. However, reliance upon technology also opens new vulnerabilities. For example, the national attention and impact of the failure of just one communications satellite "was a stark demonstration of the vulnerability of technology and just how dependent we have become on instant communication."[2] The United States military is by no means immune

to this dependence upon technology and the associated vulnerabilities. In fact, current defense spending constraints that are pushing the services to make greater use of commercial systems may magnify these vulnerabilities. Military organizations must adapt in order to minimize the risks associated with reliance upon technology, and especially information technology.

A Revolutionary Structure?

Many view the increasing military use of information technology as a revolution in military affairs. However, as Professor Andrew Krepinevich, Jr. points out, "technological change by itself is insufficient to bring about a military-technical revolution. Innovative operational concepts and organizational innovations designed to exploit new technologies are crucial to a military's ability to realize large gains in military effectiveness."[3] Therefore, one of the most important questions arising from the perceived information revolution in military affairs is how forces should be organized to take best advantage of the vast potential gains promised by IO. Any such structure must fully exploit the opportunities presented by offensive information operations and, perhaps more importantly in the near term, defend friendly information and associated systems from exploitation and attack.

The recently released joint IO doctrine describes organizations that closely reflect the current structure.[4] However, there have been proposals to restructure the typical joint force information operations structure to include a separate component commander for information similar to those for the air, land, and maritime components.[5] In fact, at the urging of the United States Navy's Second Fleet, the United States Atlantic Command has advocated and tested the concept of a separate information warfare component

commander in exercises.[6] This proposal is intriguing, but close examination reveals that creating separate a joint force information component with its own component commander is not a viable way to implement IO in the joint operations.

Structure for Discussion

The first requirement in any discussion of IO is to have a common understanding of the terminology involved. The presentation of this research begins by defining information operations and other related terms and concepts germane to the dialog that follows. While this paper assumes a basic familiarity with typical joint force organization, it provides a brief overview of the current joint force IO cell structure.

Once the foundation has been laid, the next step is defining how a distinct information component might be organized under a separate component commander. This includes an overview of assets that could be considered information assets, and a comparison of the information component's role compared to those of the more traditional components. This new component structure is based upon forces currently fielded or envisioned to be available in the near future according to available open-source information.

The problems arising from implementation of a joint force information component commander fall into two areas. The first is the failure of the separate information component structure to adhere to two time-proven principles of war, unity of command and simplicity. The other area shows that concentrating IO functions in a theater component is not the most appropriate level to provide maximum IO benefits to the joint force. The information threat transcends traditional physical boundaries, and requires a broad view beyond any one theater to be most effective. Finally, before recapping the

findings of this research, alternatives for organizing and employing IO are outlined, though their full development exceeds the scope of this investigation.

Notes

[1] Joint Pub (JP) 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, cover.

[2] "Galaxy 4 satellite not expected to be restored," *CNN*, 20 May 1998, n.p.; on-line, Internet, 9 February 1999, available from http://cnn.com/TECH/space/9805/20/satellite. update/index.html.

[3] Andrew F. Krepinevich, Jr., "The Military-Technical Revolution: A Preliminary Assessment," in *War Theory,* ed. Gwen Story and Sybill Glover, (Maxwell AFB, AL: Air Command and Staff College, September, 1998), 34.

[4] JP 3-13, IV-1.

[5] Jeffrey R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010*, (Maxwell AFB, AL: Air University Press), 4.

[6] "Joint Force Information Warfare Component Commander," Air Force Doctrine Center, n.p.; on-line, Internet, 28 January 1999, available from http://www.usafdoctrine. maxwell.af.mil/ do/i%26i/issues/jfiwcc.htm.

Chapter 2

Foundation for Discussion

In an era of increasing conflicts that decry the use of conventional military means, words (or terminology) have never played a more important role.

—Tom Barrows, Joint Warfighting Center
"Terminology," *A Common Perspective*

The term information operations means something to almost everyone in the military. However, the meanings tend to differ substantially due to the relative infancy of the field and the newness of joint definitions for IO. To many, the idea of information operations is limited to computer systems, hacking, and the like. Others include almost any function that generates, moves, or uses information in their definition. The need for a common set of definitions for IO is brought home by the Defense Science Board. In its report about defending against information warfare, one of the seven major observations is that the lack of standard terminology makes solving difficult issues even more challenging.[1] For the purposes of this paper, definitions are taken from Joint Pub 3-13, Joint Doctrine for Information Operations. In order to facilitate the discussions that follow, the important definitions are highlighted here.

Information Operations Defined

Joint Pub 3-13 defines information operations (IO) as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[2] The tremendous scope encompassed by this definition becomes apparent in light of the joint definition of information and information systems. Information is defined as "facts, data, or instructions in any medium or form."[3] An information system is "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[4] Thus, the vision of IO in the joint arena is not limited to computer systems. In fact, IO can be interpreted as applying to virtually any aspect of warfare. Such things ranging from the maps and charts carried by troops on the front lines to the ideas in the minds of leaders of both sides fall within the purview set forth by these definitions.

Another term commonly found in discussions of information and the military is information warfare (IW). While this may generate a great deal of confusion, the difference between IO and IW is actually very simple—"IW is IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[5] Thus, IW includes both the offensive and defensive portions of IO. IO will be used to refer to IO and IW throughout this paper except when IW is specifically to be addressed to the exclusion of non-conflict information operations.

Service Perspectives on Information Operations

Looking at current doctrine of the services illustrates the lack of common definitions in the United States military regarding information operations and warfare. The variances in IO definitions have contributed to the differing service viewpoints regarding

IO. Even as the joint definitions are adopted, it requires time for them to make their way into standard usage.

Air Force. Air Force IO doctrine was published 5 August 1998, just two months before Joint Pub 3-13, Joint Doctrine for Information Operations. In its glossary, Air Force Doctrine Document 2-5, Information Operations, includes what has become the joint definition, but goes on to state:

> "the Air Force believes that a more useful working definition is: [*Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare.*]"[6] (emphasis from original)

In the Air force definition it is IW, not IO that takes on offensive and defensive components. In addition, the joint definition for information warfare is listed in the AFDD 2-5 glossary, but the body contradicts the joint definition by stating that defensive IW is "conducted across the spectrum from peace to war."[7] Under the joint definitions given above, that would be defensive IO.

Army. The Army's IO doctrine is listed in Field Manual 100-6, Information Operations. The FM 100-6 definition of IO is similar to the joint definition, and includes both offensive and defensive components of IO. The Army IO doctrine includes most of the elements included in the joint definition, though many are lumped in the somewhat limiting category of command and control warfare (C2W) where their targets are more strictly focused towards defeating the enemy command and control (C2) system, while defending friendly C2. The joint view expressed in JP 3-13 applies these capabilities to any part of the friendly or adversary systems that use, produce, or deliver information, not strictly command and control systems. However, as systems become more

integrated, distinguishing C2 systems from other systems may become increasingly difficult.

Navy. The Navy has not yet published a dedicated IO doctrine document. IO as covered in Navy Doctrine Publication 6, Naval Command and Control, begins to address the concept of information warfare in the context of command and control.[8] Much like the Army, the Navy presently concentrates on the C2W subset of the overall IO picture, calling it "the military strategy that implements information warfare on the battlefield."[9] The Navy has begun exploring implications of IO in the broader sense, and is deeply involved in devising new and better methods of executing current C2W operations.[10]

Marine Corps. The Marines clearly focus "the human dimension of the conflict, with the objective of maximizing human and operational flexibility instead of relying on technology to minimize friction."[11] This does not mean, however that they do not recognize the potential value of employing IO. Marine Corps Order 3430.8, Policy for Information Operations, directs development of IO doctrine and focuses Marine IO offensive actions on C2 targets at the operational and tactical levels of war.[12] It goes on to emphasize the importance of information defense and IO training but notes that IO will not "completely replace time-tested operational techniques."[13]

Elements of Information Operations

Given the breadth of IO, it is useful to subdivide it into different elements. Perhaps the most obvious first subdivision is between offensive and defensive IO. This distinction is similar to that of other military capabilities and areas of interest, such as the offensive and defensive division in counterair. According to joint doctrine, offensive IO seeks "to affect adversary decision makers and achieve or promote specific objectives."[14]

Logically, "defensive IO integrate and coordinate policies, operations, personnel, and technology to protect and defend information and information systems."[15]

Within this framework we can begin to characterize the widely varied components of IO more logically. In the offensive IO realm, JP 3-13 includes such assigned and supporting activities as: operations security (OPSEC), military deception, psychological operations (PSYOP), public affairs (PA), civil affairs (CA), electronic warfare (EW), physical attack/destruction, special information operations (SIO), and, potentially, computer network attack (CNA).[16] All of these activities are mutually supported by intelligence.[17] These capabilities cover a diverse spectrum of traditional and developing military capabilities. Because they are not traditional disciplines, a couple of these areas require further explanation to ensure clarity. Special information operations are "information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security . . . require a special review and approval process."[18] Computer network attack could potentially overlap with SIO since it is "operations taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the networks themselves."[19]

The defensive side of IO is no more constrained than its offensive counterpart and is made up largely of the capabilities designed to counter those of offensive IO. The capabilities associated with defensive IO include information assurance (IA), operations security (OPSEC), physical security, counterdeception, counterpropaganda, public affairs, counterintelligence (CI), electronic warfare (EW), and special information operations (SIO).[20]

There are a few basic ideas relevant to the conduct of information operations that will be important in discussing the need for a separate information component commander in the JTF structure. From a military perspective, it is clear that the components of IO included in the Joint Pub 3-13 require coordination with almost every element of the joint force. As an illustration, consider Figure 1 which depicts the current doctrinal joint force IO structure. The figure makes clear the vast amount of coordination required with other parts of the joint force. However, the figure fails to emphasize that effective integration of IO into joint military operations demands detailed planning and tremendous coordination with other United States government organizations.[21] This, in turn, makes it clearer that IO may not be as easily confined within a specific AOR as traditional military means.

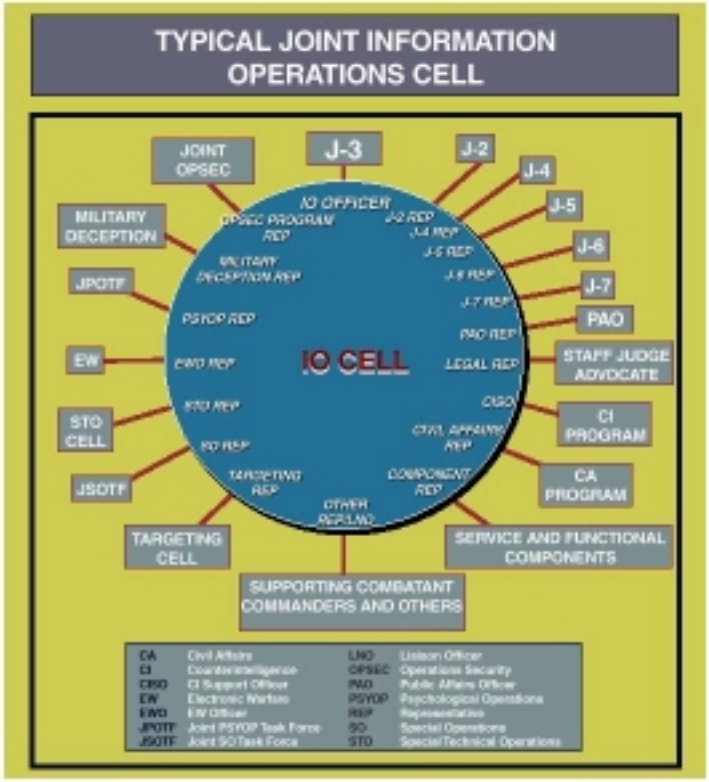

Figure 1. Current joint IO structure (JP 3-13)

One final definition will make the following discussions easier. When referring to a separate component commander for information operations the term Joint Information Operations Component Commander (JIOCC) will be used to highlight the responsibility of this individual integrating IO. Other options put forth in the literature include Joint Force Information Component Commander (JFICC)[22] and Joint Force Information Warfare Component Commander (JFIWCC).[23] In light of the approved joint definitions relating to IO, the former is too unclear and broad, while the latter unnecessarily restricts the component commander to operations relating to times of crisis. In fact, Joint Pub 3-13 points out that IO "may have their greatest impact on influencing an adversary decision maker in peacetime and the initial stages of a crisis."[24]

Notes

[1] Defense Science Board (DSB), Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D), November 1996, n.p.; on-line, Internet, 28 November 1998, available from http://jya.com/iwdmain.htm.

[2] JP 3-13, I-9, GL-7.

[3] JP 3-13, I-9, GL-7.

[4] JP 3-13, I-11,GL-7.

[5] JP 3-13, I-11.

[6] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 5 August 1998, 41.

[7] AFDD 2-5, 2, 42.

[8] Naval Doctrine Publication 6, *Naval Command and Control*, 19 May 1995, n.p.; on-line, Internet, 10 January 99, available from http://ndcweb.navy.mil/Ndp6/ndp60001.htm.

[9] Dan Kuehl, "Joint Information Warfare: An Information-Age Paradigm for Jointness," *Institute for National Security Studies Strategic Forum*, Number 105, March 1997, n.p.; on-line, Internet, 22 November 98, available from http://www.ndu.edu/inss/strforum/forum105.htm.

[10] Kuehl, n.p.

[11] Kuehl, n.p.

[12] Marine Corps Order (MCO) 3430.8, *Policy for Information Operations*, 19 May 1997, 4.

[13] MCO 3404.8, 4.

[14] JP 3-13, I-10.

[15] JP 3-13, I-10.

Notes

[16] JP 3-13, viii, II-6.
[17] JP 3-13, viii.
[18] JP 3-13, GL-10.
[19] JP 3-13, GL-5.
[20] JP 3-13, I-10, III-7.
[21] JP 3-13, IV-1.
[22] Barnett, 4.
[23] "Joint Force Information Warfare Component Commander," n.p.
[24] JP 3-13, II-7.

Chapter 3

Organizing Joint Forces with an Information Component Commander

> *The teams and staffs through which the modern commander absorbs information and exercises his authority must be a beautifully interlocked, smooth-working mechanism. Ideally, the whole should be practically a single mind.*
>
> —General Dwight D. Eisenhower
> Joint Pub 0-2

Studies and exercises examining the impact of information operations upon military operations have revealed the necessity for a single point of contact for IO.[1] The challenge for the joint force commander is to organize IO forces to have the desired central contact without negatively impacting other capabilities or components. Joint Pub 0-2, Unified Action Armed Forces (UNAAF), notes that JFCs "have the authority to establish functional component commands to control military operations."[2] One proposal is to establish a joint force information operations component commander (JFIOCC). This chapter investigates how information forces could be organized under a JFIOCC structure and how such a structure might impact employment of the overall joint force.

What Constitutes the Information Component?

In his book, *Future War: An Assessment of Aerospace Campaigns in 2010*, Jeffrey A. Barnett states that in conflicts the JFC should name a joint force information

component commander (a form of the JFIOCC) "responsible for fighting and winning the information campaign."[3] Barnett assigns five goals to this new component commander

1. Collect information on enemy capabilities, deployments, and intentions.
2. Fuse data collected from all sources and distribute timely, filtered information to users.
3. Flow friendly information efficiently in the face of enemy attacks and competing friendly requirements.
4. Degrade enemy information networks.
5. Defend friendly information networks against enemy intrusion.

In pursuit of these goals, Barnett envisions routinely giving the JFIOCC operational control (OPCON) over some forces. In addition, he envisions temporary transfer of OPCON over forces normally under the OPCON of other component commanders.[4]

In the traditional military structure, it is relatively clear what constitutes an air, land, or maritime component force. Even special operations forces can be relatively easily differentiated. At the current level of maturity of IO, however, information forces are much more difficult to delineate. The joint definition of IO is so broad one could consider virtually any military capability to be an information system, and thus fall under the information component under the JFIOCC's control. Indeed, it is difficult to imagine a military capability that does not either collect, process, store, transmit, display, disseminate, and act on information. Clearly, such an overarching definition is not useful or practical. More practically, forces over which the JFIOCC would logically exercise OPCON are outlined below based upon the various IO capabilities they represent.

The most obvious JFIOCC forces would be those conducting special information operations and, if developed, computer network attack capabilities. This would likely result in the need for detailed coordination with the special technical operations (STO) organization of the joint force. It is even possible that a merger of the STO function with

the JFIOCC structure would make sense, though that is beyond the scope of the discussion.

OPSEC is the responsibility of every soldier, sailor, marine, and airman. However, it is very reasonable for the IO component to include those forces dedicated to monitoring compliance and designing programs for educating the troops of the dangers of failing to observe proper OPSEC procedures. OPSEC becomes even more important with the proliferation of new, and often poorly understood, means of communication in everyday use. Facsimile machines, wireless communications of all types, to include cellular telephone, and, of course, electronic mail and the Internet provide rich sources for adversary exploitation unless robust training and monitoring programs are in place.

PSYOP forces provide another key IO capability that would fit under the JFIOCC. Most of the forces for conducting PSYOP reside with the five active and eight reserve PSYOP battalions under the United States Army Special Operations Command. The Air Force Special Operations Command also possesses EC-130E Commando Solo psychological operations broadcasting platform.[5] Implementation of a JFOICC would supercede the need for the joint psychological operations task force (JPOTF). PSYOP also fulfills, along with PA, the defensive IO capability of counterpropaganda.

PA capability is another capability, similar to OPSEC, that must be distributed throughout the joint force. However, the JFIOCC could control the overall PA policy guidance and the JFC's own PA tasks. By combining supervisory PA function with the other information hubs of the JFIOCC, security of operations could be protected while ensuring consistency of information disseminated by the joint force.

Another IO capability focused on perception management is deception. Though there are restrictions upon military deception deliberately targeting the United States public, media, or decision-makers, deception operations seek to mislead the enemy regarding friendly intentions, capabilities and the like in order to contribute to achievement of friendly objectives. Such operations must also be closely coordinated with CA, PA, and PSYOP to avoid conflicts and achieve the maximum positive effect.[6] The JFIOCC structure provides a nearly ideal forum for coordination of all of these efforts. Diverse forces not under OPCON of the JFIOCC may be called upon to conduct deceptions, but the forces planning deception strategy should be under the JFIOCC's direct control.

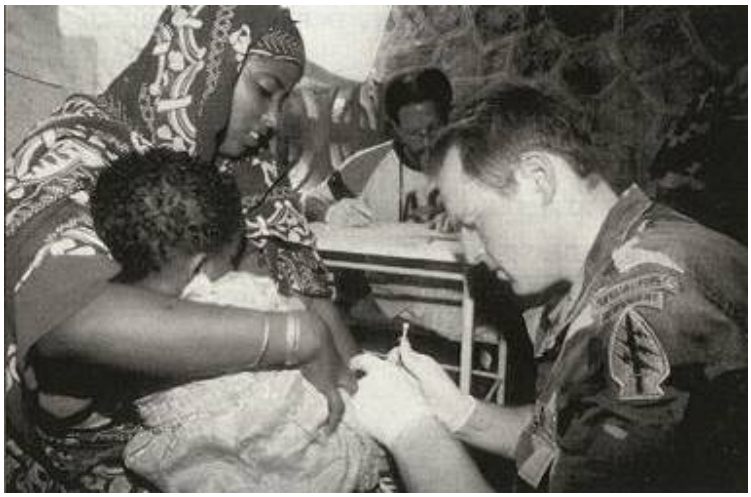

Figure 2. USSOCOM medic working in Eritrea (USSOCOM)

As indicated by their coordination with perception management capabilities just described, CA is closely related to PA, PSYOP, and deception. CA "activities range from advice and assistance to welfare, stability, and security of friendly governments and their population."[7] Currently, United States Special Operations Command possesses one active Army battalion devoted to CA with the vast majority of its capability coming from the reserve component (see Figure 2). The Marines maintain some CA trained active

personnel and can conduct CA activities with reserve augmentation. The JFIOCC should control all dedicated CA units and devise policies to guide all other forces that may engage in CA activities to maximize the coordination with the overall joint force effort.

A capability readily associated with IO is EW. EW is made up of three components, electronic warfare support (ES), electronic protection (EP), and electronic attack (EA). ES supports by identifying and locating enemy systems and capabilities, performing battle damage assessment, providing warning and even identifying potential sources for the enemy to gain intelligence on friendly assets.[8] All services have some level of ES capability, from the transportable land-based systems employed by the Marines and the Army to airborne assets such as the Air Force RC-135, Navy EP-3 and ES-3, Army RC-12 and EH-60. Other national ES assets may also be employed by the JFIOCC. Means of EP include deconfliction of friendly use of the electromagnetic spectrum, employment of equipment and techniques aimed at denying enemy exploitation of friendly systems (encryption, spread spectrum, etc.), and even self protection jamming.[9] EP-associated forces likely to fall under the JFIOCC are predominantly limited to planning and organizing functions, since many EP techniques must be employed by traditional forces in the conduct of their primary mission. Probably the most well known EW subdivision is EA. Ground-based jamming systems employed by Army and Marine forces combine with airborne jamming assets such as the Air Force's EC-130E Compass Call and the Navy's EA-6B Prowler (Figure 3). In addition, EA includes physical attack of an enemy's means of exploiting the electromagnetic spectrum with anti-radiation missiles, other conventional munitions, and, potentially, directed-energy weapons.[10]

Figure 3. EA-6B jamming aircraft fires HARM missile (JP 3-13.1)

Physical attack is also an overall IO capability, extending to targets beyond those falling under the EW umbrella just described. Such attacks may be any attack on a target that supports IO objectives by any type of munitions or platforms. Because of this, selecting specific capabilities that would fall under JFIOCC OPCON is not easy. Likely candidates would include anti-radiation missile assets (the so-called HARM-shooters, see Figure 3) and special capabilities such as the now well-known carbon filament carried by Tomahawk cruise missiles attacking the Iraqi electrical power system during the opening flurry of Operation Desert Storm.[11] In addition, the rapid technological development commonplace today may create new classes of nontraditional weapons focused on attacking information technology dependent systems. If and when such weapons are developed and fielded, the JFIOCC would be the component commander to exercise operational control over them.

Finally, returning to the first of Barnett's goals outlined above, the question of integrating some or all of the intelligence functions with the JFIOCC must be addressed. Many of the information assets listed above contribute substantially to the joint force's understanding of the enemy force's capabilities and intentions. A Defense Science Board

task force report observed that "information warfare has been particularly troublesome for the intelligence community."[12] Merging the intelligence function into the information component could help resolve some of these difficulties, but could create new problems, too. The Air Force proposes a concept of information-in-warfare to integrate not only intelligence, but also navigation, weather, and communication capabilities into IO.[13] A full discussion of this aspect of IO is beyond the scope of this paper, but it is likely that such an integration would not adhere to the principles of war as discussed in the next chapter.

Notes

[1] DSB, n.p.
[2] JP 0-2, IV-18.
[3] Barnett, 10.
[4] Barnett, 10.
[5] United States Special Operations Command, *United States Special Operations Forces Posture Statement*, 1998, 48-49, 53, 57.
[6] Joint Pub 3-58, *Joint Doctrine for Military Deception*, 31 May 1996, V, I-3, I-4.
[7] Joint Pub 3-57, *Doctrine for Joint Civil Affairs*, 21 June 1995, vii.
[8] Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, 7 February 1996, II-5 – II-7.
[9] JP 3-13, II-5.
[10] JP 3-13.1, II-6
[11] Michael R. Gordon, and General Bernard E. Trainor, *The General's War*, (Boston: Little, Brown and Company, 1995), 216.
[12] DSB, n.p.
[13] AFDD 2-5, 2.

Chapter 4

Principles of War and the JFIOCC

Know the enemy and know yourself; in a hundred battles you will never be in Peril.

—Sun Tzu
The Art of War

The JFIOCC concept seeks to address the need to reorganize the military structure to better accommodate the changes brought about by the incorporation of IO into everyday military operations. However, the JIOCC concept is not an appropriate organization for integrating IO into joint warfare. Based upon the discussion in the preceding chapter, it is clear an IO component would take numerous forces from other components and that there are many cases where the lines between IO and more traditional operations are blurred. Current doctrine views IO as a force enabler that should be integrated in all components, rather that isolated. This perception is echoed in a congressional committee report that states, information operations "is a key 'enabler' to achieve superiority on future battlefields."[1] Because the JFIOCC concept attempts to focus what should be a common, distributed capability into a single command, it conflicts with the time tested principles of war that are "the enduring bedrock of US military doctrine."[2] Specifically, the JFIOCC violates the principles of unity of command and simplicity.

Unity of Command

As defined in Joint Pub 3-0, "unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose."[3] The forces under the operational control of the JFIOCC as outlined in the preceding chapter draw heavily from those currently assigned to other, more traditional component commanders. Difficulty arises because most of those forces are critical to the ability of the other component commanders to conduct their own operations. Many of the assets that could fall under the control of the JFIOCC provide are also multi-role systems that have valuable missions not necessarily related specifically to information operations.

Examples demonstrate the difficulties that could be encountered when organizing forces with a separate information component. The area of physical attack is one where the conflicts become readily apparent. Suppose the JFC chooses to use air forces to destroy a vital enemy C2 node that is hardened and heavily defended against air attack. Of course there are a number of potential attack strategies, but for this illustration, consider a typical aircraft strike package. The primary strikers would be equipped with precision-guided munitions for attacking the target and would carry self-protection jammers for defense. EA in the form of support jamming for the package is required in the form of EA-6B and possibly EC-130 Compass Call aircraft. Threat updates would be provided by ES EP-3 or RC-135 aircraft, and fighter support and air aerial refueling will be needed for most of the aircraft. With the structure defined in Chapter 3, the JFIOCC has OPCON of the ES and EA aircraft, while the joint force air component commander,

or JFACC, exercises OPCON over the strike and refueling platforms. Thus even a fairly typical strike effort violates the joint doctrine call for a single responsible commander.

The situation is even more blurred when assigning operational control of multi-role systems. Recall the Tomahawk missiles with the special carbon fiber payload mentioned above. While that payload logically falls under JFIOCC OPCON, what happens when the warhead of the same missile is switched out for a conventional high-explosive payload? Does the missile jump back and forth between OPCON of the JFIOCC and the JFMCC (joint force maritime component commander) based upon the current warhead? Does control again go to the JFIOCC if the target is a C2 node? Clearly that is impractical as well, especially when compounded by the fact that the missile is deployed aboard a ship or submarine belonging to the JFMCC (or, potentially, one of the JFACC's aircraft). This is not even the most extreme example. Consider an attack aircraft configured with a combined load of conventional bombs, air-to-air missiles, and anti-radiation missiles. The JFACC and JFIOCC cannot share OPCON of the aircraft. Does OPCON (or even simply tactical control) depend upon whether the target is an "information" target? If so, what constitutes and information target? Is a bridge carrying electrical power supply cables to a C2 site in a city center a conventional or information target? Prosecution of such a synergistic attack could be delayed or even avoided because of confusion or parochialism even though attacking the bridge and the electrical supply supports the JFC's overall goals.

A related danger from reassigning forces from existing components to the JFIOCC is the strong likelihood that loss of those forces could result in the losing commander giving up capabilities required to successfully conduct normal operations for which he or she is

responsible. The example of the strike package demonstrates this problem. If the JFACC had to use manned aircraft to attack a hardened, heavily defended facility without the support of forces under control of the JFIOCC, the success of the attack, particularly within loss tolerances, is unlikely.

Simplicity

The JFIOCC structure also goes against the principle of war of simplicity. Simplicity is highly desirable in planning and organizing military forces and their activities. With all else equal, simpler is better when conducting joint operations. As emphasized in Joint Pub 3-0, Doctrine for Joint Operations, "Simplicity and clarity of expression greatly facilitate mission execution . . . and are especially critical to mission success."[4] The vagaries of delineating IO from more traditional operations causes complexity as demonstrated in the unity of command examples just described. Air Force Doctrine Document 1, Air Force Basic Doctrine, emphasizes that "straightforward plans and unambiguous organizational and command relationships" are central to reducing complexity of military operations.[5] Multi-role systems in a joint force that includes a JFIOCC clearly violate simplicity due to the ambiguous nature of their assignment as discussed previously.

Notes

[1] House, Excerpt from *House Report 105-132 on Defense Authorization for 1998, Title II – Research, Development, Text [sic] and Evaluation*, n.p.; on-line, Internet, 22 November 1998, available from: http://www.jya.com/hr105-132.txt.

[2] JP 3-0, A-1.

[3] JP 3-0, A-2.

[4] JP 3-0, A-3.

[5] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine,* 21.

Chapter 5

The Unbounded Theater

There is no geography or sanctuary in cyberspace.

—Vice Admiral Arthur Cebrowski
Grand Strategy for Information Age National Security

The JFIOCC concept focuses too narrowly on the JFC's area of responsibility (AOR) to best employ IO in support of the joint force. National structures with a broader view provide better IO support to the JFC for three reasons. First, defensive IO requires detailed coordination on a global scale to be most effective. Second, rapid execution of some sensitive information operations may be expedited by having a rapid capability to obtain direct approval of senior leaders. Finally, joint forces will increasingly rely on forces and capabilities deploying or operating from the United States and elsewhere outside the theater. This will create new vulnerabilities best protected by an organization not limited to a theater.

Need for a Broader View

One of the biggest problems with defense against an information attack may be recognizing that such an attack is underway. An adversary could launch a series of seemingly unrelated information attacks against US infrastructures or information systems, military or civilian, from a number of seemingly benign locations worldwide.

Especially if conducted in the "cyber" realm, such attacks could simply be written off as "glitches," and not even noted as an attack. As an example of the problem, participants in a RAND Corporation war game were unable to reach a consensus understanding of the threat posed when a number of information attacks were conducted against United States and allied targets.[1]

Taking a number of seemingly unrelated events and merging them together to identify a coordinated attack upon the United States requires a single, globally focused, national organization.[2] Presidential Decision Directive 63 (PDD 63), issued in May 1998, recognizes this need for a single point-of contact with a national perspective by authorizing a "national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[3] In addition it proposes a national information sharing center to coordinate with the private sector. The Defense Science Board proposes similar notion for Department of Defense-related issues.[4]

In addition, the Defense Science Board (DSB) gives some of the underlying reasons for such a national structure. It notes that "information warfare has been particularly troublesome for the Intelligence Community because IW is a non-traditional intelligence problem."[5] Because of this, the board continues, IW capability "is not easily discernable by traditional intelligence methods."[6] IO will require a new type of far more highly trained and educated, and thus scarce, collectors and analysts.[7] The scarcity of the appropriately qualified personnel is another strong argument for a more single national point of contact.

Recently, the Department of Defense has taken action in line with the PDD 63 and DSB recommendations. In December 1998, a Joint Task Force for Computer Network

Defense was created "to coordinate and direct defense of all DOD computer networks and systems."[8] In order to be most effective, jurisdictional and efficiency considerations mandate that JTF CND coordinate its efforts with other government agencies and, ideally, with the private sector. Regardless of its final form, JTF CND demonstrates that DOD has recognized that isolating information defense in theaters does not provide the global coordination needed for effective information defense. The creation of JTF CND may also be the foundation for a national structure coordinating the full spectrum of IO.

Political Sensitivities

The preceding section shows that there are compelling reasons to defensive information operations on a global scale. The sensitivities surrounding many offensive operations enhance the case for a single defensive IO organization and make a case for a similar offensive IO structure. In addition, combining national offensive and defensive IO structures may result in synergies benefiting both sides of the IO picture.

The defensive issues revolve around the restrictions prohibiting the military from taking certain actions within the United States (the Posse Comitatus Act).[9] The speed with which events may occur in the information age require an organization in close and reliable contact with other government agencies. In addition, a central defensive IO organization would be in a better position to coordinate with law enforcement agencies and the NCA in determining if or when a situation crosses the threshold of constituting an attack upon the United States. One example of a complex enforcement issue made headlines recently. In September, 1998, activists attempted to disable an Internet site operated by the Pentagon by attempting to overload it with requests. The Pentagon turned the attack around by sending graphics and messages back to the offending systems

in such a high volume that those systems crashed. The incident sparked debate over whether or not the response was legal and ethical.[10] Not only do questions arise regarding the appropriateness of the response, but also whether the response fell within the purview DOD or another agency.

Political considerations regarding offensive use IO also require a national coordinating organization. One of the roles would be coordinating rules of engagement (ROE) regarding IO employment. In addition, some offensive IO actions will likely require NCA approval. A national organization with access to the JCS and NCA would ensure accurate understanding by senior leaders of the proposed operations and by the military of the intent of the approval. One justification for top-level approval of certain information operations is that some information operations, especially "cyber attacks," could traverse unknown paths through neutral nations to arrive at the target. This could be viewed as a violation of sovereignty akin to over-flying a nation, without permission, to attack an adversary. A more important reason for this high-level authorization stems from the same interdependence that creates vulnerability for the United States. IO attacks have the potential for creating large cascading effects. These cascading effects make IO very effective, but also increase the potential for widespread, and/or unintended, consequences. Such effects cause some nations may view certain IO efforts as being comparable to use of weapons of mass destruction.

Thus, political sensitivities reinforce the case for a single national military organization responsible for coordinating IO functions. Restrictions on military operations inside the United States require close coordination with other agencies to ensure effective defensive IO efforts. This coordination is best done by a single, co-

located organization. Offensive IO requires creation of a centralized body to set overall national ROE for IO. More importantly, such an organization is needed to clearly, quickly, and effectively coordinate employment of the more sensitive IO capabilities with national leadership.

Global Vulnerabilities

The justification for national coordinating organizations for IO in the two preceding sections may seem to lose the focus on IO for joint forces. However, all of the areas covered above directly impact the JFC. The decreased size and forward presence of US military forces requires that future operations will be more closely tied to the continental United states for two reasons. First, a large proportion of the forces made available to the JFC will need to be deployed from the United States to the AOR. Second, in an effort to reduce the logistics requirements of deploying forces, many capabilities will remain stateside. Theater forces will exploit information technology to reach back to these organizations remaining in the continental United States. These two factors will create new vulnerabilities for the JFC's forces that are best addressed by national rather than theater-based IO organizations.

Deployment. With more and more forces expected to deploy or operate from the United States, the attractiveness of US domestic targets as an asymmetric means of influencing operations in the AOR will grow tremendously. A major source of vulnerabilities arises from the heavy reliance upon domestic commercial infrastructure beyond the control of the military. A startling example of this growing dependency is that "95% of DOD communications are supported by commercial infrastructures."[11] Even after allowing that some portion of that is for administrative communications not

directly impacting the JFC, the number is staggering. However, communications are not the only area where the military relies heavily on civilian infrastructure.

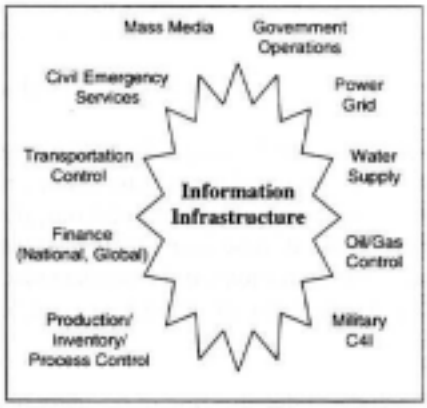

Figure 4. Infrastructure interdependence (DSB Report)

At the same time domestic commercial infrastructures are growing in military significance, their very nature is changing as the result of competitive pressures. Infrastructures are becoming more centrally controlled, highly automated, and dependent upon information technology.[12] The result is greater interdependence of seemingly unrelated infrastructures, with the information infrastructure forming the bonds between them (see Figure 4). This increasing interdependence, in turn, means that "except in rare instances, isolation of military, national, public, and private information systems is all but impossible today."[13] The central role of information infrastructure and blurring of divisions secure a vital role in overall infrastructure protection for military IO.

An example of how this directly impacts the JFC is included in the 1996 report of the Defense Science Board Task Force on Information Warfare – Defense. In researching the report, the task force learned that

> points of failure had been identified for each of three infrastructures (telecommunications, power, transportation) supporting a key port city in the United States. If these individual locations were attacked or destroyed,

> or in the case of power or telecommunications, if the resident electronics were disturbed, it would impact the ability of military forces to deploy at the pace specified in the Time Phased Force Deployment List.[14]

Obviously, the inability of the JFC to get forces as rapidly as planned can create substantial vulnerabilities to the forces in theater. The JFIOCC structure can do little to protect this aspect of the JFC's forces. Instead, a single, overarching IO organization working in close coordination with theater IO forces better serves the need of the JFC.

Reachback. One solution to the vulnerabilities stemming from the need to deploy forces forward is to rely on technology to allow deployed forces to exploit capabilities remaining in the rear. General Henry H. Shelton, Chairman of the Joint Chiefs of Staff, describes the concept as using "superior data connectivity to move electrons, not people."[15] The advantage of this so-called reachback "will become increasingly important for reducing the deployment footprint, thus preserving critical lift."[16] It also reduces the number of troops directly exposed to enemy action in the theater. The Air Force tested the concept in September 1998 at EFX 98 by using "video teleconferencing, the Internet, radios, telephones, and other means of data transmission" to connect a simulated deployed location at Eglin AFB, Florida with Langley AFB, Virginia.[17]

The heavy reliance of the JFC on reachback makes the case that IO organizations supporting the JFC should not be theater-centric. Reducing deployed forces reduces some vulnerabilities while creating others. Though he was writing specifically about air forces, *Air Force Magazine* Senior Editor John Tirpak was on target for all joint forces when he wrote that "an enemy able to cut off the flow of information being passed back and forth from CONUS [continental United States] could achieve significant disruption of the AEF's operations."[18] Such a disruption could occur anywhere in the information path from the rear location through the forward theater forces. Because of this, the JFC is

better served by a single IO organization capable of working with the entire supporting information system, rather than relying on a theater-centric JFIOCC structure.

Impact on Joint Force Organization

The explosion of information technology means that "the distinction between 'front lines' and 'rear areas' will be blurred beyond recognition."[19] For the JFC, this makes the implementation of a successful IO structure particularly challenging. For a number of reasons, the JFC's best option for IO organization includes a national organization, rather than a JFIOCC focused more narrowly on the theater. First, decentralization of IO reduces efficiency and effectiveness of detecting information attacks, and dilutes the scarce, highly-specialized defensive IO resources. Second, the political sensitivity of some IO methods calls for a central point of contact by which efforts may readily be coordinated with other agencies. In addition, sensitive information operations may require national-level approval, which can be facilitated by a central organization with ready access to, and an established relationship with, the approving authorities. Finally, the increased use of forces deployed and employed from the United States opens new vulnerabilities which extend beyond theater boundaries. Taken together, these three areas show that the JFIOCC is not the best means for employing IO for joint forces due to a theater view in a realm where geographic boundaries have little impact.

Notes

[1] Lt Col Kevin J. Kennedy, USAF, Col Bruce M. Lawlor, USARNG, and Capt Arne J. Nelson, USN, *Grand Strategy for Information Age National Security: Information Assurance for the Twenty-first Century*, (Maxwell AFB, AL, Air University Press, August, 1997), 8.

[2] DSB, n.p.

Notes

[3] "WHITE PAPER: The Clinton Administration's Policy on Critical information Infrastructure Protection: Presidential Decision Directive 63" May 22, 1998.

[4] DSB, n.p.

[5] DSB, n.p.

[6] DSB, n.p.

[7] DSB, n.p.

[8] Daniel Verton and L. Scott Tillett, "DOD confirms cyberattack 'something new,'" *CNN*, 6 March 1999, n.p.; on-line, Internet, 6 March 1999, available from http://www.cnn.com/TECH/computing/9903/06/dod.hacker.update.idg/index.html/

[9] Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 23 March 1994 (as amended through 12 January 1998), 338.

[10] Winn Schwartau, "Cyber-vigilantes hunt down hackers," *CNN*, 12 January 1999, n.p.; on-line, Internet, 12 January 1999, available from http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/.

[11] LCDR Andy Wilde, "Update: Information Operations," *A Common Perspective: USACOM Joint Warfighting Center's Newsletter*, 6, No. 2 (October 1998): 8.

[12] Wilde, 9.

[13] Richard E. Hayes and Gary Wheatley, "Information Warfare and Deterrence" *Institute for National Strategic Studies Strategic Forum*, Number 87, October 1996, n.p.; on-line, Internet, 22 November 1998, available at http://www.ndu.edu/inss/strforum/forum87.html.

[14] DSB, n.p.

[15] General Henry H. Shelton, "A Word from the New Chairman," *Joint Forces Quarterly*, Autumn/Winter 1997-98, 6.

[16] John A. Tirpak, "The Long Reach of On-Call Airpower," *Air Force Magazine* 81, no. 12 (December 1998): 25.

[17] Tirpak, 24.

[18] Tirpak, 26.

[19] Krepinevich, 37.

Chapter 6

Alternatives to the JFIOCC

> *This is not the end. It is not even the beginning of the end. It is, perhaps, the end of the beginning.*
>
> —Winston Churchill
> *Oxford Dictionary of Quotations*

The JFIOCC is not the best structure for conduct of joint force information operations because of unity of command issues, inordinate complexity, and a focus too narrowly centered on the theater. All three of these issues may adversely impact other operations and operations overall. Before concluding, it is appropriate to investigate very briefly some potential alternatives to the JFIOCC proposal. The concepts and constructs discussed below have not been investigated in detail, and certainly require further study beyond the scope of this effort to evaluate them in detail.

Theater Forces . . .

Conventional Forces. It is clear that simplicity and unity of command are best served leaving most theater forces under the appropriate "traditional" component commanders—air, land, maritime, and special operations. Those forces are most effective against information and non-information targets when operated in a highly integrated manner, rather than "stove-piped" in an information component. Information

operations, both offensive and defensive, must operate across all war fighting disciplines to be most effective

Special Operations. Removing such capabilities from the information component structure outlined previously leaves potential IO-specific capabilities that operate in the so-called "cyber realm" and the numerous coordination functions under the JFIOCC. A substantial portion of those unique IO capabilities are likely come under the rubric of "special information operations," SIO. The Joint Pub 3-13 definitions and concepts of IO and SIO overlap substantially with the Joint Pub 1-02, Department of Defense Dictionary of Military and Associated Terms, definition of special operations:

> Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or *politically sensitive areas*. These operations are *conducted during peacetime competition, conflict, and war*, independently or in coordination with operations of conventional, nonspecial operations forces. *Political-military considerations frequently shape special operations*, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in *degree of physical and political risk, operational techniques, mode of employment*, independence from friendly support, and *dependence on detailed operational intelligence* and indigenous assets.[1] (emphasis added)

Thus, those SIO capabilities deployed to the JFC's AOR logically fit with the rest of the special operations capability under the joint force special operations component commander (JFSOCC).

Advocacy and Coordination. This integration of forces into the traditional component makes the JFIOCC's information component primarily a coordinating element with essentially no forces. That is somewhat like the current structure of the IO cell described by Joint Pub 3-13 and touched on earlier. Advocacy for, and prosecution

of, IO concepts and targets is a serious concern in a joint force structure without a JFIOCC structure. One means of ensuring IO concerns are given fair consideration is to assign primary responsibility for IO cell to an officer of comparable rank to the component commanders. This IO boss takes responsibility for nominating and advocating IO targets via the joint targeting coordination board or other comparable structure used by the JFC. This individual would also be able to identify went the desired targeting effects for other nominated targets matched with IO capabilities. To ensure theater IO efforts exploit and are consistent with national efforts, the senior IO officer requires a larger staff with authority to coordinate directly with the national-level IO organizations.

. . . Tied to National Structures

As indicated in the previous chapter, events and organizations outside the JFC AOR are equally important to the JFC's accomplishment of his or her objectives. An overarching national IO structure is required. The establishment of national military structures such as those described by the DSB are key to accurate threat assessment and development of IO warning capability.[2] Alone, however, their efforts will be of limited success. The military must take a leading role in the interagency effort and in developing relationships with the private sector as outlined by PDD 63. From the perspective of the JFCs, support of the national structures is a mandatory force protection measure. This support could be focused through the chief of the JFC's IO cell.

Perhaps the single most effective means of increasing IO effectiveness of joint forces, and the military as a whole is through education. Joint Pub 3-13 emphasizes that IO needs to be integrated into all operations to be most effective.[3] The simple idea that

there needs to be an advocate for IO in the joint force structure demonstrates that not all commanders understand the huge potential payoffs offered by proper integration of IO and the potential vulnerabilities it opens. The more commanders, troops, government agencies and the private sector understand about the capabilities and vulnerabilities inherent in IO, the more effective IO efforts will be. From the military perspective, IO must be integrated professional military education at all levels. IO should also be integrated into exercises more completely to the extent that classification allows.

Final Words

Anytime a new technology enters the military, there is a need to ensure appropriate organizations are established to fully exploit the potentially large gains the technology offers and protect against new vulnerabilities it presents.[4] The JFIOCC concept is a valuable idea for looking at the conduct of IO under the JFC, but it is not the best organization for the state-of-the-art of today's military forces. As stated in Joint Pub 3-13, "IO should be an integral part of all joint military operations."[5] From the offensive perspective, organizing all IO assets into a single component is not practical due to the varied capabilities of today's weapon systems and the ability of almost any force to engage at least some IO targets. On the defensive side, all military organizations produce, use, and/or distribute information. Thus every military unit must be responsible for protecting its information and related systems.

IO also opens new horizons that extend beyond strictly military bounds. The JFIOCC is too restrictive and tied to tradition limited geographic views of the theater of operations. As Vice Admiral Cebrowski stated, cyberspace overwhelms the bounds of geography and leaves no sanctuary. Thus JFCs must be involved in the national IO effort

when considering or conducting theater operations. As efforts to reduce the forward "footprint" continue, key pieces of the JFC's force will be located outside the AOR. However, out of sight cannot mean out of mind in this case. Force protection must extend to all forces the JFC requires to continue the mission, whether they are deployed to the theater, mobilizing to deploy, or remaining stateside but linked electronically to the theater batttlespace.

Notes

[1] JP 1-02, 404.
[2] DSB, n.p.
[3] JP 3-13, I-3.
[4] Krepinevich, 34.
[5] JP 3-13, IV-1.

Glossary

Acronyms

AEF	aerospace expeditionary force
AOR	area of responsibility
C2	command and control
C2W	command and control warfare
CA	civil affairs
CI	counterintelligence
CNA	computer network attack
CND	computer network defense
DOD	Department of Defense
DSB	Defense Science Board
EA	electronic attack
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
HARM	High-speed anti-radiation missile
IA	information assurance
IO	information operations
IW	information warfare
JCS	Joint Chiefs of Staff
JFACC	joint force air component commander
JFC	joint force commander
JFICC	joint force information commander
JFIOCC	joint force information operations commander
JFIWCC	joint force information warfare commander
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JFSOCC	joint force special operations component commander
JP	Joint Pub
JPOTF	joint psychological operations task force
JTCB	joint targeting coordination board

NCA	National Command Authorities
OPCON	operational control
OPSEC	operations security
PA	public affairs
PDD	Presidential Decision Directive
PSYOP	psychological operations
ROE	rules of engagement
SIO	special information operations
STO	special technical operations
US	United States
USAF	United States Air Force
USSOCOM	United States Special Operations Command

Definitions

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (Joint Pub 3-13)

civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Also called CA. (Joint Pub 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02)

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective

C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. (This term and its definition modifies the existing term and its definition and are approved for inclusion in the next edition of Joint Pub 1-02.)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. a. cryptosecurity — The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. transmission security — The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. emission security — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security — The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations.(Joint Pub 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (Joint Pub 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

defensive information operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Joint Pub 3-13)

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic

attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams, or antiradiation weapons). b. electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronic intelligence. (Joint Pub 1-02)

information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (Joint Pub 3-13)

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Joint Pub 3-13)

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. (Joint Pub 3-13)

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack. (Joint Pub 3-13.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

physical security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (Joint Pub 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA. (Joint Pub 1-02)

special information operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO. (Joint Pub 3-13.)

special operations--Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. These operations are conducted during peacetime competition, conflict, and war, independently or in coordination with operations of conventional, nonspecial operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called SO. (Joint Pub 1-02)

Bibliography

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine,* September 1997.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations,* 5 August 1998.

Barnett, Jeffrey R. *Future War: An Assessment of Aerospace Campaigns in 2010*. Maxwell AFB, AL: Air University Press, 1996.

Barrows, Tom. "Terminology." *A Common Perspective: USACOM Joint Warfighting Center's Newsletter* 6, no. 2 (October 1998): 32.

Defense Science Board, Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D), November 1996, n.p. On-line. Internet, 28 November 1998, available from http://jya.com/iwdmain.htm.

"Galaxy 4 satellite not expected to be restored," *CNN*, 20 May 1998, n.p. On-line. Internet, 9 February 1999, available from http://cnn.com/TECH/space/9805/20/ satellite.update/index.html.

Gordon, Michael R., and General Bernard E. Trainor. *The General's War.* Boston: Little, Brown and Company, 1995.

House, Excerpt from *House Report 105-132 on Defense Authorization for 1998, Title II – Research, Development, Text [sic] and Evaluation.* On-line. Internet, 22 November 1998, available from: http://www.jya.com/hr105-132.txt.

"Joint Force Information Warfare Component Commander," Air Force Doctrine Center, n.p. On-line, Internet, 28 January 1999, available from http://www.usafdoctrine. maxwell.af.mil/ do/i%26i/issues/jfiwcc.htm.

Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 23 March 1994 (as amended through 12 January 1998).

Joint Pub 3-58. *Joint Doctrine for Military Deception,* 31 May 1996.

Joint Pub 3-57. *Doctrine for Joint Civil Affairs,* 21 June 1995.

Joint Pub 3-13. *Joint Doctrine for Information Operations,* 9 October 1998.

Joint Pub 3-13.1. *Joint Doctrine for Command and Control Warfare (C2W),* 7 February 1996.

Hayes, Richard E. and Gary Wheatley. "Information Warfare and Deterrence" *Institute for National Strategic Studies Strategic Forum,* Number 87, October 1996, n.p. On-line, Internet, 22 November 1998, available at http://www.ndu.edu/inss/strforum/ forum87.html.

"Information Warfare: An Old operational concept with new implications." *Institute for National Security Studies Strategic Forum*, Number 99, November 98. On-line. Internet, 22 November 1998, available from http://www.ndu.edu/inss/strforum/forum99.htm.

Kennedy, Lt Col Kevin J. USAF, Col Bruce M. Lawlor, USARNG, and Capt Arne J. Nelson, USN. *Grand Strategy for Information Age National Security: Information*

Assurance for the Twenty-first Century. Maxwell AFB, AL, Air University Press, August, 1997.

Krepinevich, Andrew F., Jr. "The Military-Technical Revolution: A Preliminary Assessment." In *War Theory*. Edited by Gwen Story and Sybill Glover. Maxwell AFB, AL: Air Command and Staff College, 1998.

Kuehl, Dan. "Joint Information Warfare: An Information-Age Paradigm for Jointness." *Institute for National Security Studies Strategic Forum*, Number 105, March 1997, n.p.; on-line, Internet, 22 November 98, available from http://www.ndu.edu/inss/ strforum/forum105.htm.

Naval Doctrine Publication 6, Naval Command and Control, 19 May 1995, n.p. On-line, Internet, 10 January 99, available from http://ndcweb.navy.mil/Ndp6/ ndp60001.htm.

The Oxford Dictionary of Quotations, 3rd ed. (Oxford: Oxford University Press, 1979).

Schwartau, Winn. "Cyber-vigilantes hunt down hackers," *CNN*, 12 January 1999, n.p. On-line. Internet, 12 January 1999. Available from http://www.cnn.com/TECH/ computing/9901/12/cybervigilantes.idg/.

General Henry H. Shelton, "A Word from the New Chairman," *Joint Forces Quarterly*, Autumn/Winter 1997-98.

Singer, Abe and Scott Rowell, "Information Warfare: An Old Operational Concept with New Implications," *Institute for National Strategic Studies Strategic Forum*, Number 99, December 1996, n.p. On-line. Internet, 22 November 98. Available from http://www.ndu.edu/inss/strforum/forum99.htm.

Tirpak, John A. "The Long Reach of On-Call Airpower," *Air Force Magazine* 81, no. 12 (December 1998): 20-26.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Wilde, LCDR Andy, "Update: Information Operations," A Common Perspective: USACOM Joint Warfighting Center's Newsletter, 6, No. 2 (October 1998).

United States Special Operations Command, United States Special Operations Forces Posture Statement, 1998

"WHITE PAPER: The Clinton Administration's Policy on Critical information Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998.